Cisco - CCIE

Written Training Program

International Network Services

A Study Guide for The New CCIE Routing and Switching Qualification Exam

As of September 1999

Thomas Schiller

This preparation guide was written to assist anyone who is going to take the CCIE R/S written test. In July of 1999 Cisco updated the CCIE R/S written test, so be careful about the date of the study documents used when preparing for this exam. This document should be **ONLY** used as a guide for studying, do not expect to read this and go pass the exam.

According to the Cisco blue print located on CCO the test covers the following areas:

1) Cisco Device Operation:
2) General Networking Theory:
3) Bridging & LAN Switching:
4) Internet Protocol (IP):
5) IP Routing Protocols:
6) Desktop Protocols:
7) Performance Management:
8) WAN: (addressing, signaling, framing)
9) LAN:
10) Security:
11) Multi-service:

The sections below try to follow the blue print, and provide the associated material from various sources. Most of the information has been copied from the Cisco Documentation CD, RFC's, or Caslow's Cisco Certification book, but if you find a discrepancy please let me know.

Details

Test number: 350 – 001
There are 100 multiple choice and multiple answer questions. No fill in the blanks! It appears that each test pulls from a database of questions, as opposed to the old style of test 1, test 2... You have 2 hours to complete the exam, this amount of time is ample for the test. If you feel rushed you need to prepare more!

Passing score is 65%

IMHO, the test had several "bad" questions that had no correct answers. So passing score is more around 70% to accommodate for the 3 to 5 "bad" questions. You can add comments to those questions you deem "bad". I don't know what Cisco does with the comments. I have complained about tests before, and they are less then interested in fixing the tests.

1) Cisco Device Operation:

Commands: show, debug
Infrastructure: NVRAM, Flash, Memory & CPU, file system, config reg
Operations: file transfers, password recovery, Simple Network Management Protocol (SNMP), accessing devices, security (passwords)

Password recovery with incomplete answers-
Reboot router, break, set conf reg, skip setup mode, change / erase passwords

Flash storage
Show flash - field values –
To eliminate any files from Flash memory (invalidated or otherwise) and free up all available memory space, the entire Flash memory must be erased; individual files cannot be erased from Flash memory. D means deleted but not erased.

config reg x102

Configuration Register Boot Values

Boot Value	**Description**
0x100	Sets the boot field to binary 0000, which configures the system to boot manually; initiated by using the **b** command at the ROM monitor prompt.
0x101	Sets the boot field to binary 0001, which configures the system to boot automatically, using configuration information stored in read-only memory.
0x102 to 0x10F	Set the boot field to binary 0010 to 0111, which configures the system to boot automatically using the **boot system** commands in nonvolatile memory. (These values set the boot field to binary 0010-111.) If there are no **boot system** commands in nonvolatile memory, the system uses the configuration register value to form a filename from which to netboot a default system image stored on a network server. (Refer to the appropriate hardware guide for details on default filenames.)

How many ways to initially configure a router?

- SNMP – no
- Console with setup – yes
- Console with entering full config – yes
- Console for base config then TFTP – yes
- Bootp/ RARP config - yes

When a frame is sent to a full transmit queue what happens? Output drop

Limit SNMP access? Snmp-server **Community**

Sending a break to the router during normal operation cause the router to reload, is this a problem?
Hardware problem

2) General Networking Theory:

OSI model: Layer comparisons, functions
General Routing Concepts: Split horizon, difference between switching and routing, summarization, Link State vs. Distance Vector, loops, tunneling
Protocol comparisons: Internet Protocol (IP) vs. Internetwork Packet Exchange (IPX), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), etc.
Standards: 802.x, protocol limitations
Protocol Mechanics: Windowing/Acknowledgements (ACK), fragmentation, maximum transmission unit (MTU), handshaking, termination

Retransmission of frame after line hit on Frame or HDLC is up to (router or host)?

Reliable transport – TCP LLC2?

802.3 ether type = FFFF
802.2 DSAP/ SSAP question – verify

Protocol IPX 0 Ethernet_802.3
Protocol IPX E0 Ethernet_802.2
Protocol IPX 8137 Ethernet_II
Protocol IPX 8137 Ethernet_SNAP

Understand LLC2 - Logical Link Control, type 2. Connection-oriented OSI LLC-sublayer protocol. Logical Link Control. Higher of the two data link layer sublayers defined by the IEEE. The LLC sublayer handles error control, flow control, framing, and MAC-sublayer addressing. The most prevalent LLC protocol is IEEE 802.2, which includes both connectionless and connection-oriented variants.

Understand packet sequencing and acknowledgement.

The destination MAC of a frame that has to go across a router? The MAC of the router

A couple questions about hosts and servers not being able to talk across routers. All should be due to improper default gateway settings on the hosts.

3) Bridging & LAN Switching:

Transparent Bridging: IEEE/DEC spanning tree, translational, Configuration Bridging Protocol Data Unit (BPDU), Integrated Routed and Bridging (IRB), Concurrent Routing and Bridging (CRB), access lists
Source Route Bridging: Source-route translational bridging (SR/TLB), source-route transparent bridging (SRT), data-link switching (DLSw), remote source-route bridging (RSRB), access lists
LAN Switching: Trunking, VLAN Trunk Protocol (VTP), inter-switch link (ISL), Virtual LANs (VLANS), Fast Ether Channel (FEC), Cisco Discovery Protocol (CDP), Cisco Group Management Protocol (CGMP)
LANE: LAN Emulation Client (LEC), LAN Emulation Server (LES), Broadcast and Unknown Server (BUS), LAN Emulation Configuration Server (LECS), Simple Server Replication Protocol (SSRP)

VTP types – server, client, transparent

RIF fields and RSRB virtual ring questions

RSRB requires the virtual ring to be the same, watch for decimal to hex conversions. vring 19 does not equal vring x19!

Taken from www.studygroup.com :

In Token Ring, What is a RIF and how do I read it?

The RIF or Routing Information Field in Token Ring is a map through the network for bridging beyond the current ring. The RIF shows the path from the originating ring to the destination ring with a path consisting of ring, bridge combinations.The RIF directly follows the source address in the frame when present.

The first bit of the Source Address is the Routing Information Indicator (RII) and is 0 for frames not leaving the ring and 1 for frames leaving the ring and having a RIF. (If the MAC address is 10 00 5a 12 34 56 then the source address will appear as 90 00 5a 12 34 56 for a frame with a RIF.) In the IBM version which is implemented by Cisco and most other vendors the maximum number of ring-bridge combinations in the RIF is 8 or a maximum of 7 hops. The last bridge will always be shown as 0.

The information contained in the RIF consists of the Routing Control Field (2 Bytes) and multiple Route Designation Fields (each 2 bytes).

****

Routing Information Field (RIF)
RCF RD RD RD ...
2 Bytes 2 Bytes 2 Bytes 2 Bytes ... (min of 2 Bytes, max of 18 Bytes total)
RCF = Routing Control Field
RD = Route Designator Field

****

The Routing Control Field (RCF) consists of five subfields:

****

Routing Control Field (RCF)

	Byte 0:	Byte 1:
bit	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
	B B B L L L L L	D F F F R R R R

B = Broadcast Indicators
L = Length Bits (length of RIF)
D = Direction Bit
F = Largest Frame Bits
R = Reserved Bits (always 0)

****

Broadcast Indicators (3 bits)
0xx Non Broadcast
10x all-routes Broadcast
11x Single route Broadcast (spanning explorer)

Length of the RIF (5 bits)
The length must be an even number between 2 and 18. (IEEE 802.5 allows for a longer RIF but 18 is the limit in all field implementations)

Direction Bit (1 bit)
0 read left to right
1 read right to left

Largest Frame Bits (3 bits)

000	up to 516 bytes
001	1500
010	2052
011	4472
100	8144
101	11407
110	17800
111	used in all-route broadcast frames

Reserved Bits (4 bits)
Transmitted as 0's

Route Designator Field
The Route Designator Field consists of two subfields:
Ring Number (12 bits) values between 0x001 and 0xfff (1 to 4095 decimal)
Bridge Number (4 bits) values between 0x1 and 0xf (1 to 15 decimal)
****

Route Designator Field (RD)

```
          Byte 0          Byte 1
bit   0 1 2 3 4 5 6 7   0 1 2 3 4 5 6 7
      R R R R R R R R   R R R R B B B B
```

R = Ring Number (12 bits)
B = Bridge Number (4 bits)
****
Another very good resource that deals with RIFs in extreme detail is: IBM Token-Ring Network Architecture Reference, SC30-3374-02, Sep 1989

Examples (all RIFs in hexidecimal):

RIF 1: C8 10 00 11 1f 41 00 20
This indicates a single route broadcast frame with a RIF of 8 bytes with a maximum frame size of 1500 bytes. The path is read left to right as ring 1 bridge 1 to ring 500(0x1f4) bridge 1 to ring 2. This is a two hop path.

The RIF is often written as C810 001 1 if4 1 002 0 to make the ring, bridge combination easier to read. Note that rings here are expressed in hexidecimal but must be configured in cisco routers by the decimal equivalents (that is, 500 not 1F4).

RIF 2: 1290 001 1 1f4 1 002 2 300 1 034 2 2f2 3 003 1 f00 0
This RIF indicates a non broadcast frame with a RIF of 18 bytes with a maximum frame size of 1500 bytes with the path read from right to left. The path is ring 3840(0xf00) bridge 1 to ring 3 bridge 3 to ring 754 (0x2f2) bridge 2 to ring 52 (0x34) bridge 1 to ring 768 (0x300) bridge 2 to

ring 2 bridge 1 to ring 500 (0x1f4) bridge 1 to ring 1. This RIF is the maximum length allowable and goes thru 7 bridges (hops).

SSRP- ATM / Does all equipment need to be Cisco? Yes but works with 3rd party LEC's

Transparent bridging

Transparent from token to eth –the MAC change to canonical
Broadcast address of BPDU - The Destination Address field indicates the destination address as specified in the Bridge Group Address table. For IEEE Spanning-Tree Protocol BPDU frames, the address is 0x800143000000. For IBM Spanning-Tree Protocol BPDU frames, the address is 0xC00000000100. For Cisco Spanning-Tree Protocol BPDU
frames, the address is 0x800778020200.

ISL – Cisco proprietary, FastE or GigE and token ring to connect multiple switches

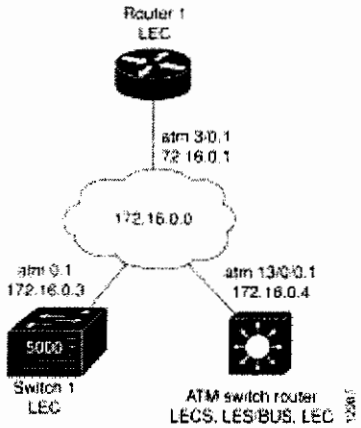
CGMP –
Multicast transmission can be implemented at both the data link layer (layer 2) and the network layer (layer 3).

Cisco offers a solution to this inefficiency by allowing the "smarts" of a Cisco router running Cisco IOS software to communicate with a Catalyst switch to better manage IP multicast distribution at layer 2. The answer is the CGMP, Cisco Group Multicast Protocol.

As its name implies, CGMP is a Cisco-developed protocol that allows Catalyst switches to leverage IGMP information on Cisco routers to make layer 2 forwarding decisions. The net result is that, with CGMP, IP multicast traffic is delivered only to those Catalyst switch ports that are interested in the traffic. All other ports that have not explicitly requested the traffic will not receive it.

It is important to note here that the CGMP operation will not adversely affect layer 2 forwarding performance. Unlike other solutions that instruct the switch to "snoop" layer 3 information at the port level, CGMP preserves layer 2 switch operation. As a result, the Catalyst 5000, for example, can deliver multicast traffic at one million packets per second.

LANE – understand LANE operation



ATM Switch Router

```
ATM_Switch# show lane default-atm-addresses
interface ATM0:
LANE Client:        47.00918100000000E04FACB401.00E04FACB402.**
LANE Server:        47.00918100000000E04FACB401.00E04FACB403.**
```

```
LANE Bus:            47.00918100000000E04FACB401.00E04FACB404.**
LANE Config Server: 47.00918100000000E04FACB401.00E04FACB405.00
note: ** is the subinterface number byte in hex

ATM_Switch# show lane client
LE Client ATM0.1  ELAN name: eng_elan  Admin: up  State: operational
Client ID: 1                 LEC up for 30 seconds
ELAN ID: 0
Join Attempt: 1
HW Address: 00e0.4fac.b402   Type: ethernet          Max Frame Size:
1516
ATM Address: 47.00918100000000E04FACB401.00E04FACB402.01 - LEC

 VCD rxFrames txFrames Type      ATM Address
  0      0       0 configure 47.00918100000000E04FACB401.00E04FACB405.00 - LECS
 87      1       2 direct    47.00918100000000E04FACB401.00E04FACB403.01 - LES
 90      1       0 distribute 47.00918100000000E04FACB401.00E04FACB403.01 - LES
 91      0       1 send      47.00918100000000E04FACB401.00E04FACB404.01 - BUS
 94      0       0 forward   47.00918100000000E04FACB401.00E04FACB404.01 - BUS
```

LE_ARP

LAN Emulation Address Resolution Protocol. Protocol that provides the ATM address that corresponds to a MAC address.

CDP runs on all media that support Subnetwork Access Protocol (SNAP), including LAN and Frame Relay. CDP runs over the data link layer only.

SSCOP

atm service specific connection oriented protocol. Data link protocol that guarantees delivery of ATM signaling packets.

DLSW peer RIF question where the peers have different virtual ring numbers, and none of the answers provide a RIF field that would be close to correct.

4) Internet Protocol (IP):

Addressing: Classless Interdomain Routing (CIDR), subnetting, Address Resolution Protocol (ARP), Network Address Translation (NAT), Hot Standby Router Protocol (HSRP)
Services: Domain Name System (DNS), Bootstrap Protocol (BOOTP), Dynamic Host Configuration Protocol (DHCP), Internet Control Message Protocol (ICMP)
Applications: Telnet, File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP)
Transport: IP fragmentation, sockets, ports
Access Lists

Ip host name IP-addr IP-addr – multiple addresses can be associated with one name

One easy access-list question – make sure you know standard and extended formats.

IP crc is based on header or data or both? the entire frame

HSRP – priority high or low? And how the process works.

HSRP uses a priority scheme to determine which HSRP-configured router is to be the default active router. To configure a router as the active router, you assign it a priority that is higher than the priority of all the other HSRP-configured routers. The default priority is 100, so if you configure just one router to have a higher priority, that router will be the default active router.

The standby preempt interface configuration command allows the router to become the active router when its priority is higher than all other HSRP-configured routers in this Hot Standby group. The configurations of both routers include this command so that each router can be the standby router for the other router. The 1 indicates that this command applies to Hot Standby group 1. If you do not use the standby preempt command in the configuration for a router, that router cannot become the active router. That is to say, if a active goes down, the backup takes over and stays active until a preempt occurs.

The *Internet Control Message Protocol (ICMP)* is a network-layer Internet protocol that provides message packets to report errors and other information regarding IP packet processing back to the source. ICMP is documented in RFC 792.

UDP fragmentation - what gets fragemented? Fragmentation occurs at the IP level so...

The following discussion describes the IP packet fields.

Flags---Consists of a 3-bit field of which the two low-order (least-significant) bits control fragmentation. The low-order bit specifies whether the packet can be fragmented. The middle bit specifies whether the packet is the last fragment in a series of fragmented packets. The third or high-order bit is not used.

Fragment Offset---Indicates the position of the fragment's data relative to the beginning of the data in the original datagram, which allows the destination IP process to properly reconstruct the original datagram.

NAT

Network Address Translation. Mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space. Also known as Network Address Translator.

5) IP Routing Protocols:

Open Shortest Path First (OSPF):
Design: areas, virtual links, stub, not so stubby areas (NSSA), area border router (ABR) / autonomous system boundary router (ASBR) redistributions, media dependencies, external vs. internal, summarization
Operation: Designated Router (DR), Backup Designated Router (BDR), adjacencies, link-state advertisement (LSA) types, link-state database, shortest path first (SPF) algorithm, authentication

Border Gateway Protocol (BGP): Design: Peer Groups, Route Reflectors, Confederations, Clusters, Attributes, Autonomous Systems (AS) Operation: Route Maps, Filters, Neighbors, decision algorithm, Interior Border Gateway Protocol (IBGP), Exterior Border Gateway Protocol (EBGP)

Enhanced Interior Gateway Routing Protocol (EIGRP): Metrics, mechanics, & design
Intermediate System to Intermediate System (IS-IS): Metrics, mechanics, & design
Routing Information Protocol (RIP) & RIP v2: : Metrics, mechanics, & design
Multicast: Design, Protocol Independent Multicast (PIM - both sparse and dense), Distance Vector Multicast Routing Protocol (DVMRP), Internet Group Management Protocol (IGMP)
Access lists: distribute lists, route maps, policy routing, redistribution, route tagging

Frame / OSPF – point multipoint spokes cannot see each other. Not designated router issue… PtoM and PtoP interfaces don't have DRs.

Opsf routing configuration questions – the commands that are needed to make OSPF routing work

> Router OSPF <pid>
> Network x.x.x.x 0.0.255.255 area N

IS-IS – Link state routing

IP load balancing - **ip cef [distributed] switch**

BGP route reflector, cluster, and confederation definitions, why would you use them? Use them to minimize the IBGP configurations. The route reflector and its client peers form a cluster.

Route flap dampening –
Route flap dampening (introduced in Cisco Internetwork Operating System [Cisco IOS] Release 11.0) is a mechanism for minimizing the instability caused by route flapping. The following terms are used to describe route flap dampening:

- Penalty---A numeric value that is assigned to a route when it flaps.
- Half-life time---A configurable numeric value that describes the time required to reduce the penalty by one half.
- Suppress limit---A numeric value that is compared with the penalty. If the penalty is greater than the suppress limit, the route is suppressed.
- Suppressed---A route that is not advertised even though it is up. A route is suppressed if the penalty is more than the suppressed limit.
- Reuse limit---A configurable numeric value that is compared with the penalty. If the penalty is less than the reuse limit, a suppressed route that is up will no longer be suppressed.
- History entry---An entry that is used to store flap information about a route that is down.

A route that is flapping receives a penalty of 1000 for each flap. When the accumulated penalty reaches a configurable limit, BGP suppresses advertisement of the route even if the route is up. The accumulated penalty is decremented by the half-life time. When the accumulated penalty is less than the reuse limit, the route is advertised again (if it is still up).

CIDR – classless interdomain routing used in BGP4 only

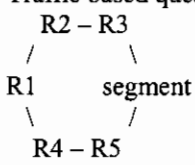
Multicast addresses –

Table 2: Well-Known Class D Addresses

Well-Known Class D Address	Purpose
224.0.0.1	All hosts on a subnet
224.0.0.2	All routers on a subnet
224.0.0.4	All DVMRP routers
224.0.0.5	All MOSPF routers
224.0.0.9	Routing Information Protocol (RIP)---Version 2
224.0.1.1	Network Time Protocol (NTP)
224.0.1.2	SGI Dogfight
224.0.1.7	Audio news
224.0.1.11	IETF audio
224.0.1.12	IETF video

Routing Policies

Traffic based question –



How do you make telnet traffic go across R2/3 and the rest of the traffic go across R4/5?

Policy-Based Routing Data Forwarding

Policy-based routing (PBR) provides a mechanism for expressing and implementing forwarding/routing of data packets based on the policies defined by the network administrators. It provides a more flexible mechanism for routing packets through routers, complementing the existing mechanism provided by routing protocols.

Routers forward packets to the destination addresses based on information from static routes or dynamic routing protocols such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF), or Enhanced Interior Gateway Routing Protocol (Enhanced IGRP®). Instead of routing by the destination address, policy-based routing allows network administrators to determine and implement routing policies to allow or deny paths based on the following:

- Identity of a particular end system
- Application
- Protocol
- Size of packets

Policies can be defined as simply as "my network will not carry traffic from the engineering department" or as complex as "traffic originating within my network with the following characteristics will take path A, while other traffic will take path B."

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/qos_c/qcpart1/qcpolicy.htm

Policy Routing Example

The following example provides two sources with equal access to two different service providers. Packets arriving on async interface 1 from the source 1.1.1.1 are sent to the router at 6.6.6.6 if the router has no explicit route for the packet's destination. Packets arriving from the source 2.2.2.2 are sent to the router at 7.7.7.7 if the router has no explicit route for the packet's destination. All other packets for which the router has no explicit route to the destination are discarded.

```
access-list 1 permit ip 1.1.1.1
access-list 2 permit ip 2.2.2.2
!
interface async 1
 ip policy route-map equal-access
!
route-map equal-access permit 10
 match ip address 1
 set ip default next-hop 6.6.6.6
route-map equal-access permit 20
 match ip address 2
 set ip default next-hop 7.7.7.7
route-map equal-access permit 30
 set default interface null0
```

BGP4, two paths from AS3 to AS5, how do you make one path have priority? setting local_pref

No routing protocol on a router, but a default route. Will the router still pass information to the next router? If so, will the next router know to send the response back to it?

Injecting 0.0.0.0 route into OSPF any considerations? Regarding ASBRs?

Autonomous System Boundary Router, ABR located between an OSPF autonomous system and a non-OSPF network. ASBRs run both OSPF and another routing protocol, such as RIP. ASBRs must reside in a nonstub OSPF area.

How do you adjust hold-down timers in a distance vector routing protocol? Timers basic yes but dangerous.

Define Split horizon.

Not sending a route advertisement back out the interface that caused the routing update

Poison reverse question does not have a correct answer, options are:

- Does not send information back out route source interface
- When route is unavailable the metric is set to infinite

Defined: Routing updates that explicitly indicate that a network or subnet is unreachable, rather than implying that a network is unreachable by not including it in updates. Poison reverse updates are sent to defeat large routing loops.

"Counting to infinity" with a distance vector routing protocol means?

This is described in more detail in RFC 1058. When topology changes, spurious routes will be introduced. The metrics associated with these spurious routes slowly increase until they reach 15, at which point the routes are removed.

Provide a solution to the problem of large routing table updates – link state protocol

Route redistribution concerns with RIP and OSPF; point out the issues to a client? One of the options is VLSM, metrics, and so on...

RIP v2 features

- Allows subnet masks
- Address-Family Identifier (AFI)---Specifies the address family used. RIP is designed to carry routing information for several different protocols. Each entry has an address-family identifier to indicate the type of address specified. The address-family identifier for IP is 2. If the AFI for the first entry in the message is 0xFFFF, the remainder of the entry contains authentication information. Currently, the only authentication type is simple password.
- Simple password - see previous
- Same 16 hop max

6) Desktop Protocols:

Internetwork Packet Exchange (IPX): NetWare Link Services Protocol. (NLSP), IPX-RIP, IPX-Service Advertising Protocol (SAP), IPX-EIGRP, Sequenced Packet Exchange (SPX), Network Control Protocol (NCP), IPXWAN, IPX addressing, Get Nearest Server (GNS), Novell Directory Services (routing & mechanisms), access lists

AppleTalk: Routing Table Maintenance Protocol (RTMP), AppleTalk Update-Based Routing Protocol (AURP), Appletalk-EIGRP, Datagram Delivery Protocol (DDP), Zone Information Protocol (ZIP), Name Binding Protocol (NBP), addressing (phase 1 & 2), access lists
DECnet/OSI: Addressing, access lists
Windows NT: NetBIOS, browsing, domain controller (e.g. WINS), access lists

Apple Talk phase 1 question, it is supported and is native if you have one cable range and one zone per range

Network/DL layer protocols that don't use resolution - i.e. IPX, CLNS

NLSP is most like IS-IS

CLNS is ISO NSAP addressing

IPX GNS is default active and forwards request to first SAP entry. If a server appears in the table with the same metric, the new server will be sent the GNS request.

IPX load balancing - **ipx max-paths 2**

AURP – appletalk update based routing – IS IT Link state... no

Route summarization – the similar bits in the network addresses are summarized.

10110101
10111001
10110111

Ip default network - ip route 0.0.0.0 0.0.0.0 *a static default route*

When default information is being passed along through a dynamic routing protocol, no further configuration is required. The system will periodically scan its routing table to choose the optimal default network as its default route. In the case of RIP, it will be only one choice, network 0.0.0.0. In the case of IGRP, there might be several networks that can be candidates for the system default. The router uses both administrative distance and metric information to determine the default route (gateway of last resort). The selected default route appears in the gateway of last resort display of the **show ip route** EXEC command.

If dynamic default information is not being passed to the router, candidates for the default route can be specified with the **ip default-network** command. In this usage, **ip default-network** takes a nonconnected network as an argument. If this network appears in the routing table from any source (dynamic or static), it is flagged as a candidate default route and is a possible choice as the default route for the router.

If the router has no interface on the default network but does have a route to it, it will consider this network as a candidate default path. The route candidates will be examined and the best one will be chosen based on administrative distance and metric. The gateway to the best default path will become the gateway of last resort for the router.

IPXWAN know what it is - IPX wide-area network, protocol that negotiates end-to-end options for new links. When a link comes up, the first IPX packets sent across are IPXWAN packets negotiating the options for the link. When the IPXWAN options are successfully determined, normal IPX transmission begins. Defined by RFC 1362.

7) Performance Management:

Traffic Management: Queuing, Weighted Fair Queuing (WFQ), Resource Reservation Protocol (RSVP), traffic shaping, load balancing

Traffic Shaping

This example shows the configuration of two traffic-shaped interfaces on a router. Ethernet 0 is configured to limit User Datagram Protocol (UDP) traffic to 1 Mbps. Ethernet 1 is configured to limit all output to 5 Mbps.

```
access-list 101 permit udp any any
interface Ethernet0
 traffic-shape group 101 1000000 125000 125000
!
interface Ethernet1
 traffic-shape rate 5000000 625000 625000
```

The following is a sample display for the show traffic-shape command for the example shown:

Router# show traffic-shape

I/F	access list	Target Rate	Byte Limit	Sustain bits/int	Excess bits/int	Interval (ms)	Increment (bytes)	Adapt Active
Et0	101	1000000	23437	125000	125000	63	7813	-
Et1		5000000	87889	625000	625000	16	9766	-

Queueing

Specify Maximum Queue Size in Bytes Example

The following example decreases queue list 9 from the default byte count of 1500 to 1400 for queue number 10:

queue-list 9 queue 10 byte-count 1400

load-interval

To change the length of time for which data is used to compute load statistics, use the **load-interval** interface configuration command. To revert to the default setting, use the **no** form of this command.

Command Mode - Interface configuration

RSVP

Resource Reservation Protocol, protocol that supports the reservation of resources across an IP network. Applications running on IP end systems can use RSVP to indicate to other nodes the nature bandwidth, jitter, maximum burst, and so forth) of the packet streams they want to receive. RSVP depends on IPv6. Also known as Resource Reservation Setup Protocol.

8) WAN: (addressing, signaling, framing)

ISDN: Link Access Procedure on the D channel (LAPD), Basic Rate Interface (BRI) / Primary Rate Interface (PRI) framing, signaling, mapping, dialer map, interface types, B/D channels, channel bonding
Frame relay: Local Management Interface (LMI), Data Link Connection Identifier (DLCI), Permanent Virtual Circuit (PVC), framing, traffic shaping, forward explicit congestion notification (FECN), backward explicit congestion notification (BECN), CIR, discard eligible (DE), mapping, compression
X.25: addressing, routing, Link Access Procedure Balanced (LAPB), error control/recovery, windowing, signaling, mapping, Switched Virtual Circuit (SVC) / Permanent Virtual Circuit (PVC), Protocol Translation

ATM: Switched Virtual Connection (SVC) / Permanent Virtual Connection (PVC), ATM Adaptation Layer (AAL), Service Specific Connection Oriented Protocol (SSCOP), User-Network Interface (UNI) / Network-Network Interface (NNI), Interim Local Management Interface (ILMI), Cell format, Quality of Service (QoS), RFC 1483 &1577, Private Network-Network Interface (PNNI), Interim-Interswitch Signaling Protocol (IISP), mapping

Physical Layer: Synchronization, Synchronous Optical Network (SONET), T1, E1, encoding
Leased Line Protocols: High-Level Data Link Control (HDLC), Point to Point Protocol (PPP), async & modems, compression
Dial on Demand Routing (DDR): dial backup

SGBP authentication failure question – source has a password failure

Several x.25 questions
A question about adding an *ip protocol map* to another router's x.121 address

One x.25 question asks for all needed configurations that must be considered
Need x.25 encapsulation
Need to set x.121 address on interface
Need to set mapping for each protocol to the dest x.121
Routing for x.25??? No, remember x.25 routing is how you set up a x.25 switch

WAN frames have what in common: flag – address – data –FCS

PPP call- the order of the steps involved in the call. LCP – PAP - NCP
Good ref:
http://www.cisco.com/warp/public/779/smbiz/service/knowledge/wan/ppp_auth.htm

What kind of HDLC compression is available? STAC
PPP compression – Stac, predictor, tcp header

For HDLC encapsulations, you can specify a Stacker compression algorithm by using the **stac** keyword. PPP encapsulations support both predictor and Stacker compression algorithms.

SONET
Synchronous Optical Network. High-speed (up to 2.5 Gbps) synchronous network specification developed by Bellcore and designed to run on optical fiber. STS-1 is the basic building block of SONET. Approved as an international standard in 1988. See also SDH, STS-1, and STS-3c.

UNI definition
User-Network Interface. ATM Forum specification that defines an interoperability standard for the interface between ATM-based products (a router or an ATM switch) located in a private network and the ATM switches located within the public carrier networks. Also used to describe similar connections in Frame Relay networks.

NNI definition

1. Network-to-Network Interface. ATM Forum standard that defines the interface between two ATM switches that are both located in a private network or are both located in a public network. The interface between a public switch and private one is defined by the UNI standard. Also, the standard interface between two Frame Relay switches meeting the same criteria.
2. Network node interface.

You must use NNI between two different vendor switches

ILMI

Interim Local Management Interface, specification developed by the ATM Forum for incorporating network-management capabilities into the ATM UNI.

IISP (interim-interswitch signaling protocol)

Interim-Interswitch Signaling Protocol, ATM signaling protocol for inter-switch communication using manually configured prefix tables. When a switch receives a signaling request, the switch checks the destination ATM address against the prefix table and notes the port with the longest prefix match. It then forwards the signaling request across that port using UNI procedures. IISP is an interim solution until PNNI Phase 1 is completed. Formerly known as PNNI Phase 0. Contrast with Dynamic IISP.

Dynamic IISP

Dynamic Interim-Interswitch Signaling Protocol, basic call routing protocol that automatically reroutes ATM connections in the event of link failures. Dynamic IISP is an interim solution until PNNI Phase 1 is completed.

9) LAN:

Datalink Layer: addressing, 802.2
Ethernet/Fast Ethernet/Gigabit Ethernet: encapsulation, carrier sense multiple access collision detect (CSMA/CD), topology, speed, controller errors, limitations, 802.3

Token Ring: token passing, beaconing, Active Monitor, ring insertion, soft & hard errors, encapsulation, topology, maximum transmission unit (MTU), speed, limitations

FDDI/CDDI: dual ring, encapsulation, class, redundancy, dual homing, medium (copper, fiber), claims, Station Management (SMT), limitations

Fast Link Pulse – Fast Ethernet negotiation

FDDI

- 4b/5b encoding? All data to be transmitted is encoded prior to transmission using a **4 of 5 group code** This means that for each 4 bits of data a corresponding 5 bit code word or symbol is generated by the encoder.
- Claim packet- if lower bid than station, packet is passed on by station. If higher bid, station forwards its own claim and bid.
- 2km on MMF between stations, 500 stations max, 200km max network diameter

Token ring bit A and bit C… A is for address recognized, and C is for frame copied. Initially 0 set to 1 once true.

What is Token Ring early release?

If early token release is supported, a new token can be released when frame transmission is complete.

What is beaconing?

A Token Ring algorithm called beaconing detects and tries to repair certain network faults. Whenever a station detects a serious problem with the network (such as a cable break), it sends a beacon frame, which defines a failure domain. This domain includes the station reporting the failure, its nearest active upstream neighbor (NAUN), and everything in between. Beaconing initiates a process called auto reconfiguration, where nodes within the failure domain automatically perform diagnostics in an attempt to reconfigure the network around the failed areas. Physically, the MSAU can accomplish this through electrical reconfiguration.

10) Security:

Authentication, Authorization, and Accounting (AAA), Terminal Access Controller Access Control System (TACACS), and RADIUS: general concepts, usage, comparisons
Firewalls: PIX, access lists, demilitarized zones (DMZ)
Encryption: public/private key, Data Encryption Standard (DES)

Radius – UDP and encryption
Tacacs – UDP and encryption
Tacacs+ - TCP and encryption

A company is connected to the Internet. What must they do to protect themselves? ACL, distribution list?

DES or encryption

Data Encryption Standard, standard cryptographic algorithm developed by the U.S. National Bureau of Standards

11) Multiservice:

Voice/Video: H.323, codecs, Signaling System 7 (SS7), Real-Time Transport Protocol (RTP), RTP Control Protocol (RTCP), Quality of Service (QoS)

Erlang B – Voice traffic unit of measure

What is H323 – video conf gateway services

SS7

Signaling System 7. Standard CCS system used with BISDN and ISDN. Developed by Bellcore.

RTP

1. Routing Table Protocol. VINES routing protocol based on RIP. Distributes network topology information and aids VINES servers in finding neighboring clients, servers, and routers. Uses delay as a routing metric. See also SRTP.

2. Rapid Transport Protocol. Provides pacing and error recovery for APPN data as it crosses the APPN network. With RTP, error recovery and flow control are done end-to-end rather than at every node. RTP prevents congestion rather than reacts to it.

**3. Real-Time Transport Protocol, one of the IPv6 protocols. RTP is designed to provide end-to-end network transport functions for applications transmitting real-time data, such as audio, video, or simulation data, over multicast or unicast network services. RTP provides services such as payload type identification, sequence numbering, timestamping, and delivery monitoring to real-time applications.

RTPCP

RTP Control Protocol, protocol that monitors the QOS of an IPv6 RTP connection and conveys information about the on-going session.

QOS

Quality Of Service, measure of performance for a transmission system that reflects its transmission quality and service availability.